Amendments to the Claims:

A listing of the entire set of pending claims (including amendments to the claims, if any) is submitted herewith per 37 CFR 1.121. This listing of claims will replace all prior versions, and listings, of claims in the application.

1.(previously presented) A record carrier having a first area storing information (data), which is at least partly stored in encrypted form (EAK(data)), this part being called an asset (EAK(data)), and which includes a first part of decryption information (HCK, EDNK(HCK)), and the record carrier further having a second area storing a second part of decryption information (UCID), wherein both the first (HCK) and second (UCID) parts of decryption information serve in decrypting the asset (EAK(data)); wherein the first area comprises a storage medium of one physical kind and the second area comprises a storage medium of another physical kind, and wherein the record carrier is designed such that both the first (HCK) and second (UCID) parts of decryption information are readable from the record carrier.

2. (cancelled)

3.(previously presented)A record carrier having a first area storing information (data), which is at least partly stored in encrypted form (EAK(data)), this part being called an asset (EAK(data)), and which includes a first part of decryption information (HCK, EDNK(HCK)), the record carrier further having a second area storing a second part of decryption information (UCID), wherein both the first (HCK) and second (UCID) parts of decryption information serve in decrypting the asset (EAK(data)); wherein the second area comprises a chip for providing the store of the second area, the chip storing a first counter (Ci) and allowing a reading and/or writing device read access to the first counter (Ci) but denying write access to it, the chip changing the value of the first counter (Ci) each time the second part of decryption information (UCID) is read by the reading and/or writing device and storing a second counter (Ce) in an encrypted form, wherein both the first (HCK) and second (UCID) parts of decryption information serve in decrypting the second counter (Ce); and wherein the payload data EAK(data) is decrypted if the second counter (Ce) coincides with the first counter (Ci).

4.(previously presented) The record carrier as claimed in claim 1, wherein

a symmetric method using a first cryptographic key, called an asset key (AK), is used for asset encryption and decryption, and

the asset key (AK) is stored in the second area in an encrypted form, wherein for its encryption a symmetric encryption method has been used, this method employing a second cryptographic key (CIDK) in whose derivation both the first (HCK) and second (UCID) parts of decryption information have been used.

5.(previously presented) The record carrier as claimed in claim 1, wherein

a third cryptographic key, called a hidden-channel key (HCK), serves in the asset decryption, and

the hidden-channel key (HCK) is obtainable from the first part of decryption information (HCK, EDNK(HCK)), the hidden-channel key (HCK) coincides with the first part of decryption information (HCK), and the first part of decryption information (HCK) is scrambled and/or encrypted within the information (data) stored in the first area.

6. (canceled)

7.(previously presented) The record carrier as claimed in claim 3, wherein

the chip is designed for checking the right of a reading and/or writing device to access the record carrier.

8.(previously presented) The record carrier as claimed in claim 1, wherein

the second area is designed for storing user-specific settings serving in controlling the access of a reading and/or writing device to the record carrier and/or in controlling manner information being read from the record carrier is presented by the reading and/or writing device to a user of the reading and/or writing device.

9. (currently amended) A device for reading from and/or writing to a record carrier, wherein the device is designed

for reading and/or writing the first part of decryption information (HCK, EDNK(HCK)) to/from the record carrier,

for reading and/or writing the second part of decryption information (UCID) to/from the record carrier,

for reading and/or writing the asset (EAK(data)) to/from the record carrier,

for obtaining complete decryption information from both the first (HCK, EDNK(HCK)) and second parts (UCID) of decryption information, and said device further comprises

a processor for decrypting and/or encrypting the asset (EAK(data)) with the complete decryption information, wherein the record carrier is designed such that both the first (HCK) and second (UCID) parts of decryption information are readable from the record carrier.

10.(previously presented) The device for reading and/or writing as claimed in claim 9, wherein the device is designed for accessing the first and second areas of the record carrier in parallel.

11.(previously presented) The device for reading and/or writing as claimed in claim 9, wherein the device is designed for storing and maintaining a revocation list of identifiers (UCID), and for at least partly refusing a user of a device access to the record carrier if the identifier (UCID) being stored on the record carrier belongs to the revocation list.

12. (cancelled)

13. (currently amended) A method for reading from and/or writing to a record carrier, comprising:

reading and/or writing the first part of decryption information (HCK, EDNK(HCK)) to/from the record carrier by a device,

reading and/or writing the second part of decryption information (UCID) to/from the record carrier by a device,

reading and/or writing the asset (EAK(data)) to/from the record carrier by a device,

obtaining complete decryption information from both the first (HCK, EDNK(HCK)) and second parts (UCID) of decryption information, and

decrypting and/or encrypting the asset (EAK(data)) with the complete decryption information, wherein the record carrier is designed such that both the first (HCK) and second (UCID) parts of decryption information are readable from the record carrier.

14. (canceled)

15.(previously presented) The device of claim 9, wherein the device is further designed

for obtaining complete decryption information from both the first (HCK, EDNK(HCK)) and second parts (UCID) of decryption information, and

for decrypting and/or encrypting the asset (EAK(data)) with the complete decryption information.

16.(previously presented) The method of claim 13, further comprising:

obtaining complete decryption information from both the first (HCK, EDNK(HCK)) and second parts (UCID) of decryption information, and,

decrypting and/or encrypting the asset (EAK(data)) with the complete decryption information.